United States General Accounting Office

GAO

Report to the Chairman, Committee on Science, House of Representatives

March 2001

INFORMATION SECURITY

Safeguarding of Data in Excessed Department of Energy Computers

GAO-01-469

Report Date *("DD MON YYYY")* 00MAR2001	Report Type N/A	Dates Covered (from... to) *("DD MON YYYY")*

Title and Subtitle INFORMATION SECURITY Safeguarding of Data in Excessed Department of Energy Computers	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) General Accounting Office, PO Box 37050,Washington, DC 20013	**Performing Organization Number(s)** GAO-01-469
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	

Abstract
The computer systems that support the Department of Energys (DOE) civilian research and development programs house enormous amounts of data and information. Although unclassified, some of the information in these systems is nevertheless sensitive and must be protected from inappropriate access or disclosure. For example, these systems might house controlled scientific and technical information such as proprietary data or information that is export controlled. For this reason, DOE property management regulations require the agency to clear the hard drives of all computers before they are transferred into the excess category for reuse or disposal. On February 16, 2001, we briefed your office on our review of the safeguarding of data in excessed DOE computers.

Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 32	

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

March 29, 2001

The Honorable Sherwood L. Boehlert
Chairman, Committee on Science
House of Representatives

Dear Mr. Chairman:

The computer systems that support the Department of Energy's (DOE) civilian research and development programs house enormous amounts of data and information. Although unclassified, some of the information in these systems is nevertheless sensitive and must be protected from inappropriate access or disclosure. For example, these systems might house controlled scientific and technical information such as proprietary data or information that is export controlled. For this reason, DOE property management regulations require the agency to clear the hard drives of all computers before they are transferred into the excess category for reuse or disposal. On February 16, 2001, we briefed your office on our review of the safeguarding of data in excessed DOE computers.

In brief, we found that DOE does not have standardized instructions, verification procedures, or training for agency and contract employees on how to properly clear excessed computers. DOE also does not ensure that procedures used to remove all software, information, and data from systems are effective. As a result, some of the excessed computers we inspected at DOE headquarters had information still stored on the hard drives.

This report officially transmits the results of our work and recommendations to assist DOE in ensuring that sensitive unclassified information is removed from excessed computers. The briefing slides, as amended, are included as appendix I.[1]

Recommendations for Executive Action

We recommend that the Secretary of Energy

- develop and implement standardized written procedures on how to effectively clear hard drives of all software, information, and data;

[1]Changes were minimal and do not affect the overall contents.

- require an independent verification that these procedures have been followed prior to turning in computers for excess to ensure that employees and contractor personnel of all DOE organizations are in compliance; and
- emphasize these procedures in the computer security training and awareness program that is required for all DOE employees and contractor personnel.

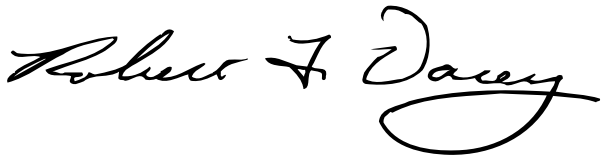
Agency Comments and Our Evaluation

In written comments on a draft of this report, which are reprinted in appendix II, DOE's Acting Director, Office of Security and Emergency Operations, concurred with our findings and recommendations. However, agency officials specifically noted that, at our exit conference, we had indicated that our inspection team found no evidence that sensitive unclassified information remained on the excessed computers at DOE Headquarters. We disagree with this statement. We wish to reiterate that in testing 26 of the approximately 700 computers that were stored at the DOE Germantown excess holding area, we identified three machines that had not been cleared. We did not thoroughly examine all of the readable text that remained on the hard drives of these computers because this was not the objective of our review. Nevertheless, as noted on our briefing slides, our spot check of these machines did reveal official correspondence and potentially sensitive cooperative research and development information.

As agreed with your office, unless you publicly announce its content earlier, we plan no further distribution of this report until 5 days from the date of this letter. At that time, we will send copies to the Honorable Spencer Abraham, Secretary of Energy, and the Honorable Mitchell E. Daniels Jr., Director, Office of Management and Budget. This report will also be available on GAO's home page at *www.gao.gov*. If you have any questions, please contact me at (202) 512-3317 or Elizabeth Johnston, Assistant Director, at (202) 512-6345. We can also be reached by e-mail at

daceyr@gao.gov and *johnstone@gao.gov*, respectively. Another key contributor to this assignment was Edward R. Alexander, Jr.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

February 16, 2001, Briefing for the House Committee on Science

Safeguarding of Data in Excessed Department of Energy Computers

Briefing for the Committee on Science
House of Representatives

February 16, 2001

Agenda

- Objectives
- Background
- Scope and methodology
- Results
- Conclusions
- Recommendations

2

Objectives

To determine whether

- DOE headquarters' excessed computers were properly cleared of sensitive unclassified information
- contractor-operated DOE facilities complied with federal regulations for excessing computers

3

Background

DOE's unclassified information systems for scientific research store enormous amounts of sensitive information, including controlled scientific and technical information, mission-essential-related information, unclassified controlled nuclear information, financial/budgetary information, and confidential personal information about employees.

4

Background (cont'd)

- In accordance with federal property management regulations and Executive Order 12999, DOE transfers useful excessed computers to other federal agencies, schools, prisons, and other nonprofit organizations and salvages those in poor condition.
- At the time of our review, about 700 computers were stored at the DOE Germantown, MD, excess holding area.

5

Background (cont'd)

- Ten DOE major field facilities reported that they have excessed about 18,500 computers in the past 2 years.
- Federal regulations require federal agencies to establish internal security procedures to ensure that sensitive unclassified information stored on the hard drives of excessed computers has been removed.

6

Background (cont'd)

- DOE's federal property management regulations require that all software (including the operating system), information, and data be cleared from computers before they are declared excess.
- The regulations further require that designated computer support personnel attach a certification tag to the equipment to indicate that the computer has been cleared of all data.

7

Background (cont'd)

- DOE's unclassified computer security program requires that employees and contractor personnel from all DOE organizations be appropriately trained.

8

Scope and Methodology

- We interviewed officials from nine DOE headquarters program offices regarding their policies and procedures for excessing computers.
- We examined a random sample of 40 computers in DOE headquarters' excess property holding area in Germantown, MD, to determine if the hard drives had been properly cleared of all software, information, and data.

9

Scope and Methodology (cont'd)

- Of the 40 computers selected for inspection, 13 had hardware problems that prevented further testing, and we were unable to read the hard drive of one because the machine's interface was incompatible with our testing software.

10

Scope and Methodology (cont'd)

- We surveyed 10 of DOE's 15 major field facilities regarding their policies and procedures for excessing computers. Our sample focused on facilities receiving substantial funding for unclassified civilian research:
  - Ames Laboratory
  - Argonne National Laboratory
  - Brookhaven National Laboratory

11

Scope and Methodology (cont'd)

- Fermi National Accelerator Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Oak Ridge National Laboratory
- Princeton Plasma Physics Laboratory
- Stanford Linear Accelerator Center
- Thomas Jefferson National Accelerator Facility

12

Scope and Methodology (cont'd)

- We conducted our work from August 2000 through November 2000, in accordance with generally accepted government auditing standards.
- We obtained DOE comments on a draft of this briefing.

13

Excessed Computers at DOE HQ Were Not Properly Cleared

- No standard procedure or guidance for properly clearing computers of software, information, and data is provided to DOE employees or contract personnel.
  - Five different contractor-developed software clearing tools were being used by the program offices that we interviewed.

14

Excessed Computers at DOE HQ Were Not Properly Cleared (cont'd)

- No office had written instructions on how to properly use the clearing tools.
- Verification procedures did not ensure that all information had been removed.

15

Excessed Computers at DOE HQ Were Not Properly Cleared (cont'd)

- Of the 26 hard drives that we could access in our sample inspection:
    - seven had the operating system software still installed.

16

Excessed Computers at DOE HQ Were Not Properly Cleared (cont'd)

- three had not been cleared of readable information and data. For example, on one machine we were able to read official correspondence as well as potentially sensitive cooperative research and development proposal information submitted by an industry partner.
- three had not been properly cleared, leaving recoverable information and data.

17

GAO
Accountability * Integrity * Reliability

DOE Facilities Were Not In Compliance

- Of the 10 facilities we surveyed,
  - one complied with federal property management regulations,
  - four used clearing processes that left data recoverable, and
  - seven did not comply with requirements for certifying that computers had been effectively cleared.

18

Conclusions

DOE does not have adequate instructions, verification procedures, and training on how to properly clear excessed computers.

DOE does not ensure that computers have been cleared or that clearing is effective.

Accordingly, computers have been excessed with information still stored on the hard drives.

19

Recommendations

To ensure that sensitive unclassified information stored on excessed computers has been removed, the Secretary of Energy should

- develop and implement standardized written procedures on how to effectively clear hard drives of all software, information, and data,

20

Recommendations (cont'd)

- require an independent verification that these procedures have been followed prior to turning in computers for excess to ensure that employees and contractor personnel of all DOE organizations are in compliance, and
- emphasize these procedures in the computer security training and awareness program that is required for all DOE employees and contractor personnel.

21

Comments From the Department of Energy

Department of Energy
Washington, DC 20585

March 14, 2001

Mr. Joel C. Willemssen
Managing Director, Information Technology Issues
United States General Accounting Office
441 G. Street, NW
Washington, D.C. 20548

Dear Mr. Willemssen:

The Department of Energy (DOE) appreciates the opportunity to review and comment on the General Accounting Office (GAO) draft report entitled "Information Security: Safeguarding of Data in Excessed Department of Energy Computers" (GAO-01-469), dated March 2, 2001. Although DOE agrees with the findings and recommendations cited in the report, I want to specifically note that at the exit briefing on February 13, 2001, your staff indicated that it had not found any evidence that sensitive unclassified information still remained on any system it reviewed during the inspection. I also want to call your attention to the efforts that are already underway in the Department to address the weaknesses identified in the report, described below and in our enclosed comments.

In the Fall of 2000, the Office of Cyber Security in the Office of the Chief Information Officer (CIO) began a major restructuring effort of the Department's cyber security policy. Since accompanying manuals and guidelines are not scheduled for completion until the summer of 2001, the CIO developed and promulgated interim guidance on many cyber topics, including sanitization.

On November 17, 2000, the Acting CIO signed a memorandum on sanitizing unclassified equipment. This memorandum reemphasized DOE Headquarters' requirements to sanitize all information technology equipment before being excessed or provided to non-government organizations such as schools. The memorandum endorsed two guidelines on sanitizing equipment issued by the National Institute of Standards and Technology and recommended that DOE sites use the aforementioned guidelines when developing their own procedures.

Enclosed is the DOE response to issues raised in the report. If you have any questions regarding the Department's comments or would like to discuss them further, please contact John Przysucha, Acting Associate CIO for Cyber Security, at 202-586-8836.

Sincerely,

Joseph S. Mahaley
Acting Director, Office of Security and
Emergency Operations

Enclosure

Printed with soy ink on recycled paper

DEPARTMENT OF ENERGY COMMENTS ON GAO DRAFT REPORT ENTITLED "INFORMATION SECURITY: SAFEGUARDING OF DATA IN EXCESSED DEPARTMENT OF ENERGY COMPUTERS"

Department Comments on Recommendations

During the past year and concurrent with GAO's review of sanitizing excessed computers, the Department of Energy (DOE) has been restructuring its security policy. DOE is intent on systematically integrating cyber security into management and work practices across the DOE complex using the approach developed in its integrated safety management program. This level of effort will include developing and promulgating new policies, orders, manuals or other guidance to support the integrated Cyber Security Management Program, and to establish the roles and responsibilities for cyber security across the Department. The Office of the CIO has developed a cyber specific management policy, DOE Policy 205.1, to systematically integrate cyber security into management and work practices at all levels predicated on a formal, organized risk management process to ensure that missions are accomplished while appropriately protecting electronic information and information systems.

Recommendation #1: Develop and implement standardized written procedures on how to effectively clear hard drives of all software, information and data.

As part of its Cyber Security Management Program, the Office of the CIO is developing a draft manual to provide detailed requirements on the content of the unclassified cyber security program. The draft manual, entitled Unclassified Cyber Security Program, describes minimum content requirements including media disposition and sanitization. The Manual will be issued in the summer of 2001 and requires each DOE site to document, as part of its cyber security program plan, procedures for:

- Media sanitization during the disposal phase of an information systems life cycle.
- Sanitizing electronic media for reuse (e.g., overwrite or degaussing of electronic media).
- Controlled storage, handling or destruction of spoiled media or media that cannot be effectively sanitized for reuse.
- Ensuring the authorized transfer of unclassified information from classified computers.
- Ensuring that need-to-know criteria are applied to personnel granted access to classified data archives.
- Verification that sanitization has been effective and complete.
- Periodic independent verification that sanitization has been completed prior to excessing DOE computers.

Recommendation #2: Require an independent verification that these procedures have been followed prior to turning in computers for excess to ensure that employees and contractor personnel of all DOE organizations are in compliance.

As discussed in the response to Recommendation #1, the Department will require, periodic independent verification that sanitization has been completed prior to turning in computers for

excess.

Recommendation #3: Emphasize these procedures in the computer security training and awareness program that is required for all DOE employees and contractor personnel.

In February 2001, the CIO issued its Cyber Security Training, Education and Awareness Program Strategy. This strategy outlines the comprehensive program under development in the Office of Cyber Security to provide cyber security training to DOE's workforce. Training in procedures to effectively sanitize information technology equipment is currently being developed as part of that program. In addition, sites are required to document their computer security awareness and training programs, which is to include training in sanitization in their site's Cyber Security Program Plan.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00